REMARKS/ARGUMENTS

1.) Claim Amendments

Claims 4,15 and 21 have been canceled. Accordingly, claims 1-3, 5-14, 16-20 and 22-33 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Niemi et al. (RFC 3310, HTTP Digest Authentication Using AKA) in view of Reiche (6,092,196), and further in view of Tuomi et al. (US 7,395,050 B2).

The Applicant extremely appreciates the Examiner's comments but respectfully traverses the rejection for the following reasons. In maintaining the Examiner's rejection, the Examiner stated that "Tuomi discloses an access controller (112) and an authentication server (114) where the authentication server creates a userID and password for the user requesting access." The Examiner then further stated that "[t]he authentication node of the instant application receives request for access and details of the temporary identity for the end user, which is similar to the functions of the access controller in the reference Tuomi." Accordingly, it is the Applicant's understanding that the Examiner is comparing the "remote server" in the present application to "authentication server" in Tuomi and the "authentication node" in the present application to the "access controller" in Tuomi.

The Applicant submits that there are a number of reasons why this argument is non-persuasive and such a comparison incorrect. First of all, as clearly recited in the present application, the remote server is the one that receives a request for access from the UE. The remote server then generates the temporary identify for the UE and sends that information to the authentication node in the UE's home network. However, in Tuomi, the access controller (112) and authentication server (114) are all within a data transfer network (118) and outside of the UE's home network (134). Accordingly, whether it is the access controller (112) or the authentication server (114) that is being compared to the authentication node as claimed in the present invention, they are not part of the UE's home network. For example, the only authentication server in the home network shown in Fig. 1 of Tuomi is the MSC/HLR (130) located in the Home Public Land Mobile Network (PLMN 134) for the mobile device (104). However, the access controller in Tuomi instead communicates with the authentication server (114) that is outside of the home network (134).

The Examiner then stated that the authentication server (114) in Tuomi is similar to the remote server in the present invention and the access controller (112) in Tuomi is similar to the authentication node in the present invention. However, as clearly shown in Fig. 1 of Tuomi, it is the access controller (112) that receives the access request from the terminal device (104) and the access controller (112) then communicates with authentication server (114) for authenticating the device. Accordingly, contrary to the Examiner's explanation, it is the access controller that is performing the access function that is similar to the remote server as claimed in the present invention. However, since the access controller (112) fails to generate a temporary identity for the UE as claimed in the present invention, the Applicant respectfully submits that Tuomi fails to anticipate or render obvious the presently pending claims.

Next, the Examiner again maintained his rejection that the Reiche disclosed or anticipated the step of "sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity of the UE." Other than showing a user's web browser sending a request to an authentication server, there is nothing in Reiche that shows a remote server sending a request to an authentication node in the UE's home network the details of the request for access wherein such request includes the temporary identity of the UE as created by the remote server. Col. 5, lines 12-22 of Reiche cited by the Examiner, for example, merely states that a user's web browser would make a contact with the central authentication server while carrying a transaction ID. However, nothing in Reiche shows a remote server sending a request to the authentication node in the UE's home network with the temporary identity of the UE as created by the remote server.

Additionally, in accordance with the teachings of the present invention, the authentication node then generates a HTTP digest challenge to the UE using an algorithm capable of generating end-user password and including details of the temporary identity of the UE and identity of said remote server. However, Niemi merely shows generating a HTTP challenge using an "AUTS" value wherein AUTS is an authentication token that has been generated by the client upon experiencing an SQN synchronization failure. Accordingly, nothing in Niemi, independently or in combination with Reiche or Tuomi, discloses or teaches the steps of (1) remote server receiving a request for access from the UE, (2) creating a temporary identity for the UE by that remote server, (3) sending to an authentication node in the UE's home network details of the request for access, said details including the temporary identity of the UE, and (4) the authentication node generating a HTTP challenge to the UE using an algorithm capable of generating end-user password including details of the temporary identity of the UE and identity of the remote server.

Also, Niemi likewise fails to anticipate or render obvious the step of "at the UE, generating a password based on the HTTP Digest Challenge, said password being associated with the identity of the remote server and the identity of the UE as created by the remote server." Since the temporary identity as created by the remote server is never received by the UE in Niemi, it cannot possibly create a password that is associated with the identity of the remote server and the temporary identity of the UE as claimed in the present invention. In Niemi, it instead uses the RAND and AUTS values to generate the "password" as clearly explained in the Examiner's cited portion of Niemi.

Therefore, the Applicant respectfully submits that all of the pending claims are patentable over the cited references and a Notice of Allowance is earnestly requested.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/John C. Han,Reg#41403/

John C. Han
Registration No. 41,403

Date: February 8, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com